Cybersecurity for Local Governments and Schools

A Weekly Cybersecurity Awareness Month Web Series

NYS COMPTROLLER
THOMAS P. DiNAPOLI

Week 4 – Tying up Loose Ends

John Horrocks, Municipal Auditor
Gerry Cochran, IT Specialist
Division of Local Government and School Accountability

NYS COMPTROLLER
THOMAS P. DiNAPOLI

Categories

- Personal, Private and Sensitive Information
- IT Asset Inventories
- Policies and Procedures
- IT Security Awareness
- Written IT Agreements
- Website Content
- Internet Use
- Malicious Software
- User Accounts and Permissions
- Passwords
- Networks and Computers
- Wireless Access
- **Physical Access**
- **Disaster Recovery**
- **Audit Trails and Logs**

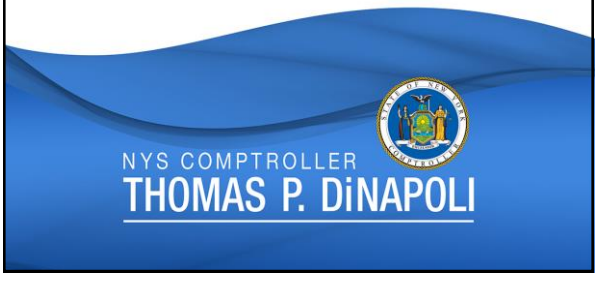
Recap - Week 3

- Networks and Computers
- Wireless Access

NYS COMPTROLLER
THOMAS P. DiNAPOLI

4

Physical Access



Physical Access

Physical controls should be in place to make sure equipment is protected. They can prevent attackers from attaining a deeper knowledge of system resources such as hardware, can limit attackers' ability to plant a device or can even stop malicious persons with destructive intent.

NYS COMPTROLLER
THOMAS P. DiNAPOLI

6

Physical Access

- Threat
  - Theft of assets
  - Misuse of resources
  - Loss of data or access

Physical Access

- Attack
  - Keylogger installation: Commack High School, New York (October 2015). A student installed a key logger device onto a classroom computer.
    - The device captured all user accounts and passwords entered into computer.
    - The student accessed an account to change grades.

Physical Access

- Best Practice
  - Restrict physical access to resources.
    - Doors and gates
    - Locks
    - Guards
  - Periodically assess physical and environmental security.
    - Smoke detectors
    - Fire alarms and extinguishers
    - Uninterruptible power supplies

Disaster Recovery

NYS COMPTROLLER
THOMAS P. DiNAPOLI

Disaster Recovery

Historically, people thought of these plans more in terms of natural disasters, such as the hurricanes that occurred in the south and the forest fires on the west coast. However, given today's computing environment with constant cybersecurity threats, having a viable contingency plan is critical if you want to recover from a computer virus or ransomware attack.

Disaster Recovery

- Threat
  - Complete data loss
  - Business process interruptions
  - Extensive resources needed for recovery

Disaster Recovery

- Attack
  - Ransomware: City of Atlanta, Georgia (March 2018).
    - Multiple municipal services were down, including databases and Wi-Fi.
    - Years' worth of data was destroyed.
    - The city initially spent $2.7 million in recovering services.

Disaster Recovery

- Best Practice
  - Develop a disaster recovery plan.
  - Distribute the plan to all responsible parties.
  - Ensure the plan is periodically tested and updated as needed.
  - Develop backup procedures.

Audit Trails and Logs

NYS COMPTROLLER
THOMAS P. DiNAPOLI

Audit Trails and Logs

Audit trails and logs contain information for events that happen within networks and systems. Examples of common logs are computer security logs that track user authentication attempts and security device logs that record possible attacks.

Audit Trails and Logs

- Threat
  - Unable to determine who accessed data or systems
  - Unable to see what was accessed
  - Unable to determine changes made to data or systems

Audit Trails and Logs

- Attack
  - Memorial Healthcare System (February 2017).
    - Protected Health Information of 115,143 individuals improperly accessed and disclosed.
    - Logs showed a former employees access used for a year with out detection and accessed 80,000 individuals .
    - Failed to regularly review records of information system activity on applications that maintain electronic protected health information.

Audit Trails and Logs

- Best Practice
  - Enable and periodically review audit logs for indications of unauthorized access or misuse of personal, private or sensitive information.
  - Install log management software if possible, and configure the system to send notifications for relevant log events.

Resources

- New York Office of the State Comptroller's Local Government Publications
  https://www.osc.state.ny.us/local-government/publications
- Center for Internet Security's Multi-State Information Sharing and Analysis Center
  https://www.cisecurity.org/ms-isac/
- New York State Office of Information Technology Services' Chief Information Security Office
  https://its.ny.gov/ciso
- United States Cybersecurity and Infrastructure Security Agency
  https://www.cisa.gov/

Thank You

Division of Local Government and School Accountability
LGSAAppliedTech@osc.ny.gov